RECEIVED
CENTRAL FAX CENTER
NOV 11 2005

CERTIFICATE OF TRANSMISSION BY FACSIMILE (37 CFR 1.8) Applicant(s): Gupta et al.			Docket No. JP920000150US1
Application No. 09/626,637	Filing Date 7/27/2000	Examiner Shin, Kyung H.	Group Art Unit 2143

Invention: METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE

I hereby certify that this Supplemental Appeal Brief (30 pages)
(Identify type of correspondence)

is being facsimile transmitted to the United States Patent and Trademark Office (Fax. No. 571-273-8300

on 11/11/2005
(Date)

Kim Dwileski
(Typed or Printed Name of Person Signing Certificate)

(Signature)

Note: Each paper must have its own certificate of mailing.

PAGE 1/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

RECEIVED
CENTRAL FAX CENTER
NOV 11 2005

Docket No. JP920000150US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Gupta *et al.*

Group Art Unit: 2143

Filed: 7/27/2000

Examiner: Shin, Kyung H.

Serial No.: 09/626,637

Title: METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL BRIEF OF APPELLANT

This Supplemental Appeal Brief, pursuant to the Office Action mailed August 11, 2005, is an appeal from the rejection of the Examiner dated August 11, 2004. The Appeal Brief filed April 11, 2005 is incorporated, in its entirety, herein by reference. The present Supplemental Appeal Brief addresses the rejections of claims in the Office Action mailed August 11, 2005.

REAL PARTY IN INTEREST

International Business Machines, Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1-6 and 11-19 are rejected. Claims 7-10 are canceled. This Brief is in support of

PAGE 2/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

an appeal from the rejection of claims 1-6 and 11-19.

STATUS OF AMENDMENTS

There are no After-Final Amendments which have not been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention discloses a method for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, but the authentication certificates of any of the server or browser are still valid. An original authentication certificate together with a server certifying authority chain (SCAC) certificate is received by the browser from the server during a SSL handshake between the browser and the server. The SCAC certificate was previously obtained by the server from the certifying authority. The browser verifies the original authentication certificate using the expired public key of the certifying authority. The browser verifies the SCAC certificate using a new public key of the certifying authority. See FIG. 1 (steps 1, 2, and 4) and specification, page 6, lines 9-10, 23-26; page 5, lines 5-10.

After verifying the original authentication certificate and after said verifying the SCAC certificate, the browser accepts the transaction between the browser and the server. See FIG. 1 (step 5) and specification, page 6, line 27 - page 7, line 2.

The SCAC certificate may be obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by: contacting the certifying

PAGE 3/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

authority using the server's private key for authentication to make a request for the SCAC certificate; verifying the request by the certifying authority using the server's public key; and generating the SCAC certificate by the certifying authority using a new private key of the certifying authority and forwarding the SCAC certificate to the server. See FIG. 2 and specification, page 7, lines 4-12.

Generating the SCAC certificate may include authenticating the server name, the server public key, old certifying authority public key, and certifying authority name. See specification, page 4, lines 24-26.

A client (CCAC) certificate may be issued by the certifying authority, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged. The CCAC certificate may be presented to the server during the handshake. See specification, page 7, lines 16-22.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1, 5-6, 11-13, and 17-19 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis et al. (U.S. Patent No. 6,233,565) in view of Weinstein et al. (U.S. Patent No. 6,094,485).

(Note: The Examiner initially stated that claims 1, 4-6, 11, 13, 17-19 are rejected over Lewis in view of Weinstein, which appears to be a typographical error in light of the claims actually analyzed by the Examiner over Lewis in view of Weinstein)

2. Claims 2, 3, 14 and 15 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable

PAGE 4/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

over Lewis-Weinstein and further in view of Perlman *et al.* (US Patent No. 6,230,266).

3. Claim 4 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis-Weinstein and further in view of Kramer *et al.* (US Patent No. 6,324,525).

4. Claim 16 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis-Weinstein and further in view of Kramer *et al.* (US Patent No. 6,324,525).

PAGE 5/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

ARGUMENT

GROUND OF REJECTION 1

Claims 1, 5-6, 11-13, and 17-19 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis et al. (U.S. Patent No. 6,233,565) in view of Weinstein et al. (U.S. Patent No. 6,094,485).

Claims 1, 5-6, 13, and 17

Appellants respectfully contend that claims 1, 6, and 13 are not unpatentable over Lewis in view of Weinstein, because Lewis in view of Weinstein does not teach or suggest each and every feature of claims 1, 6, and 13.

A first example of why claims 1, 6, and 13 are not unpatentable over Lewis in view of Weinstein is that Lewis in view of Weinstein does not teach the following first feature: "receiving an original authentication certificate **together** with a server certifying authority chain (SCAC) certificate **by the browser from the server** during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority" (emphasis added) (claim 1), and similar language for claims 6 and 13.

The Examiner cites Lewis, col. 30, lines 39-41, as disclosing the preceding first feature of claims 1, 6, and 13, except for the limitation of receiving the original authentication certificate and the SCAC certificate together.

As to the limitation of receiving the original authentication certificate and the SCAC

PAGE 6/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

certificate together, the Examiner states: "Lewis does not specifically disclose certificates received together. However, Weinstein discloses: a) receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate. (see Weinstein col. 3, lines 56-64: multiple (i.e. new, intermediate (i.e. old)) certificates within a transmission (i.e. together)) It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable multiple security client/server certificates transmitted within a network session as taught by Weinstein. One of ordinary skill in the art would be motivated to employ Weinstein in order to optimize encryption within a secure network communications session. (see Weinstein col. 2, lines 10-15: " ... provides a process and apparatus that is used by an exportable version of an SSL client ... negotiate an encrypted communication session using strong encryption with an SSL server ..."'

In response, Appellant will next argue that:

(1) the old certificate and the new certificate are not received **by the browser from the server** as required by claims 1, 6, and 13; and

(2) receiving the original authentication certificate and the SCAC certificate together does not make sense for Lewis' invention.

Appellants' analysis begins with quoting Lewis, col. 30, lines 36-50:

"**The initial CA's certificate** will be distributed by means of regular US certified mail. Included with the CA's certificate will be a hash of the next certificate key values. **When a certificate expires, the USPS certification authority will issue a new certificate** and sign it with the old certificates matching private key. The USPS CA will send a new certificate signed with the CA's new private key to the server 4. The server 4 will validate the certificate for authenticity by first checking to ensure that the new CA certificates public key authenticates the included signature. It will then hash the keys included with the new certificate to verify that the hash value match with

PAGE 7/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

the old hash included with the old CA's certificate. If both conditions validate, the old CA's certificate is deleted and replaced with a new CA certificate. " (emphasis added).

The preceding quote in Lewis demonstrates that:

(1) the old certificate and the new certificate are not received by the browser from the server as required by claims 1, 6, and 13, but are instead received by the server from the Certificate Authority; and

(2) The new certificate replaces the old certificate and thus becomes relevant only after the old certificate expires. It makes no sense for the server to receive the old and new certificates together, since the server already has possession of the old certificate when the server receives the new certificate. Thus, it is not obvious to modify Lewis to receive the old and new certificates together.

In addition, the Examiner's citation of Weinstein has no relevance for Lewis. In particular, the multiple certificates in the certificate chain described in Weinstein, col. 3, lines 54-60 are used to verify a server by a client, whereas the old and new certificates described in Lewis, col. 30, lines 36-50 are used to verify a CA certificate by a server.

A second example of why claims 1, 6, and 13 are not unpatentable over Lewis in view of Weinstein is that Lewis in view of Weinstein does not teach the following second feature: "verifying by the browser the original authentication certificate using the **expired public key** of the certifying authority" (emphasis added) (claim 1), and similar language for claims 6 and 13. The Examiner argues that Lewis discloses the aforementioned second feature of claims 1, 6, and 13. The Examiner relies specifically on content disclosed in Lewis, col. 14, lines 36-42 and col.

PAGE 8/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

30, lines 41-43.

In response. Appellants respectfully contend that Lewis col. 14, lines 36-42 does not disclose use of an expired public key as required by claims 1, 6, and 13 . Furthermore, Appellants respectfully contend that Lewis col. 30, lines 41-43 states specifically that "[t]he USPS CA will send a new certificate signed with the CA's new private key to the server" which does not even mention an expired public key. The preceding second feature requires verification by the browser using the **expired public key** of the certifying authority, which Lewis does not teach. Although Lewis discloses in col. 27, lines 10-24 that a user may verify an X.509 certificate using a CA's public key, Lewis does not teach anywhere that the browser verifies the X.509 certificate using a public key **after the public key has expired** as required by claims 1, 6, and 13.

Based on the preceding arguments, Appellants respectfully maintain that claims 1, 6, and 13 are not unpatentable over Lewis in view of Weinstein and are in condition for allowance. Since claim 5 depends from claim 1, Appellants contend that claim 5 is likewise in condition for allowance. Since claim 17 depends from claim 13, Appellants contend that claim 17 is likewise in condition for allowance.

Claims 11 and 18

Since claims 11 and 18 respectively depend from claims 1 and 13, and since Appellants have argued *supra* that claims 1 and 13 are not unpatentable over Lewis in view of Weinstein,

PAGE 9/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

Appellants maintain that claims 11 and 18 are likewise not unpatentable over Lewis in view of Weinstein.

In addition with respect to claims 11 and 18, Appellants maintain that Lewis in view of Weinstein does not teach or suggest the feature: "accepting the transaction by the browser after said verifying the original authentication certificate and after said verifying the SCAC certificate" (claim 11), and similar language for claim 18.

The Examiner argues that Lewis, col. 27, lines 10-24 teaches the preceding feature of claims 11 and 18.

In response, Appellants maintain that Lewis, col. 27, lines 10-24 teaches that a user "A" may accept a transaction after verifying an authentication certificate, but does not teach that the user "A" would accept a transaction after verifying **both** the original authentication certificate and the SCAC certificate, as required by claims 11 and 18.

Accordingly, Appellants maintain that claims 11 and 18 are not unpatentable over Lewis in view of Weinstein.

Claims 12 and 19

Since claims 12 and 19 respectively depend from claims 1 and 13, and since Appellants have argued *supra* that claims 1 and 13 are not unpatentable over Lewis in view of Weinstein, Appellants maintain that claims 12 and 19 are likewise not unpatentable over Lewis in view of Weinstein.

In addition with respect to claims 12 and 19, Appellants maintain that Lewis in view of Weinstein does not teach or suggest the feature: "wherein **obtaining** the SCAC certificate

PAGE 10/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

comprises using the new private key of the certifying authority" (emphasis added) (claim 12), and similar language for claim 19.

The Examiner argues: "Lewis disclose the method and system of claims 1, 13, wherein obtaining the SCAC certificate comprises using the new private key of the certifying authority. (see Lewis col. 30, lines 41-43: certificate (i.e. server/client) utilizing private key for digital signature generation and public key for verification)".

In response, Appellants maintain that Lewis, col. 30, lines 41-43 teaches that the CA signs the new certificate with the CA's private key. In contrast, the "obtaining" in claims 12 and 19 is performed by the server and not by the CA, as may be verified from claims 1 and 13 from which claims 12 and 19 respectively depend. In particular, claim 1 recites: "said SCAC certificate having been previously **obtained by the server** from the certifying authority" (emphasis added). Therefore, Lewis does not disclose "wherein obtaining the SCAC certificate comprises using the new private key of the certifying authority", since the CA who uses new CA's private key is not the server that obtains the SCAC certificate in accordance with claims 12 and 19.

Accordingly, Appellants maintain that claims 12 and 19 are not unpatentable over Lewis in view of Weinstein.

PAGE 11/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

GROUND OF REJECTION 2

Claims 2, 3, 14 and 15 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis-Weinstein and further in view of Perlman *et al.* (US Patent No. 6,230,266).

Claims 2 and 14

Since claims 2 and 14 respectively depend from claims 1 and 13, and since Appellants have argued *supra* that claims 1 and 13 are not unpatentable over Lewis in view of Weinstein, Appellants maintain that claims 2 and 14 are likewise not unpatentable over Lewis-Weinstein and further in view of Perlman.

In addition with respect to claims 2 and 14, Appellants maintain that Lewis-Weinstein and further in view of Perlman does or suggest not teach the following first feature: "wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key".

The Examiner states: "Lewis does not disclose a Certificate Authority (CA) that invalidates or withdraws its public/private key. However, Penman discloses Certificate Authority (CA) that invalidates or withdraws its public/private key pair through the process of revocation."

In response, Appellants note that Perlman repeatedly discusses certificate revocation. However, Perlman does not teach or suggest public key invalidation, and the Examiner has not produced a citation that allegedly discloses public key invalidation, as required by claims 2 and 14.

PAGE 12/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

In addition with respect to claims 2 and 14, Appellants maintain that Lewis in view of Perlman does not teach or suggest the second feature: "contacting the certifying authority using the server's private key for authentication **to make a request** for the SCAC certificate" (claim 2) (emphasis added), and similar language for claim 14. The Examiner argues that Perlman, col. 6, line 63 - col. 7, line 6 discloses the preceding second feature of claims 2 and 14.

In response, Appellants maintain that Perlman, col. 6, line 63 - col. 7, line 6 does not disclose "to make a request for the SCAC certificate", as alleged by the Examiner. Indeed, Perlman, col. 6, line 63 - col. 7, line 8 recites:

> "In order to update the certificates previously issued by certificate authorities 204c so as to ensure that principals relying upon such certificates now recognize the validity of certificates (including the special delegation certificate) issued by the successor CA 204b, CA 204a **may issue**, via secure off-line techniques, to certificate authorities 204c a **"renunciation" certificate** 600 (the data structure of which is represented in FIG. 6) signed using the private key of the CA 204a including information 602 stating that the CA 204a has renounced all of its certification authority (i.e., power to issue certificates), and has granted that authority to the CA 204b" (emphasis added).

Thus, Perlman, col. 6, line 63 - col. 7, line 6 discloses issuing a renunciation certificate and most certainly does not disclose requesting the SCAC certificate. In other words, "requesting" and "issuing" are different actions. Moreover, a renunciation certificate is not a SCAC certificate.

In addition with respect to claims 2 and 14, Appellants maintain that Lewis in view of Perlman does not teach or suggest the third feature: "verifying the request by the certifying authority using the server's public key" (claim 2), and similar language for claim 14. The

PAGE 13/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

Examiner argues that Perlman, col. 7, lines 15-18 discloses the preceding third feature of claims 2 and 14.

In response, Appellants maintain that Perlman, col. 7, lines 15-18 does not disclose "to make a request for the SCAC certificate", as alleged by the Examiner. Indeed, Perlman, col. 7, lines 15-18 recite: "The authorities 204c receiving such renunciation certificates from CA 204a verify that the renunciation certificates have been properly signed by the CA 204a". Appellants contend that the preceding quote of Perlman discloses verifying that the renunciation certificates have been properly signed by the CA, but does not disclose verifying the request by the certifying authority using the server's public key, as required by claims 2 and 14.

In addition with respect to claims 2 and 14, Appellants maintain that Lewis in view of Perlman does not teach or suggest the fourth feature: "generating the SCAC certificate by the certifying authority using a new private key of the certifying authority and **forwarding the SCAC certificate to the server**" (claim 2) (emphasis added), and similar language for claim 14. The Examiner argues that Perlman, col. 7, lines 12-24 discloses the preceding fourth feature of claims 2 and 14.

In response, Appellants maintain that Perlman, col. 7, lines 12-24 does not disclose "forwarding the SCAC certificate to the server" as alleged by the Examiner and as required by claims 2 and 14.

In addition, Appellants contend that the Examiner's reason for modifying Lewis by the alleged teaching of Perlman is not persuasive. The Examiner argues: "It would have been

PAGE 14/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of Lewis to include a Certificate Authority (CA) that invalidates its key pair through the process of revocation as taught in Perlman. One of ordinary skill in the art would have been motivated to incorporate the invention of Perlman in order to ensure the authenticity of certificates when a CA invalidates a public/private key pair. (see Perlman col. 2, lines 20-26: "... *network security, every principal must have a certificate ... desirable to later disable a certificate after it has been issued but prior to its expiration. For example, a principal's private key may be stolen, compromised or lost, etc. ... revoke the certificate, thereby disabling authentication via that certificate* ...")" (emphasis added)..

In response, Appellants maintain that the cited motivation in Perlman requires revocation of the original certificate ***prior to expiration*** of the original certificate. However, with respect to claims 1 and 13 from which claims 2 and 14 respectively depend, the Examiner cites Lewis, col. 30, lines 39-43 which requires that a condition precedent for issuance of the new certificate (alleged by the Examiner to be the SCAC certificate) is that the original certificate expires. See Lewis, col. 30, lines 39-43 ("**When a certificate expires**, the USPS certification authority will issue a new certificate ..." (emphasis added)).

Appellants contend that ordinary logic requires that the original certificate either have expired or not have expired (but not both) when the new certificate is issued by the CA. In other words, the Examiner is arguing to modify Lewis by the alleged teaching of Perlman by issuing the new certificate when the original certificate has both expired and not expired, which is logically impossible. Therefore, the Examiner's argument for modifying Lewis by the alleged teaching of Perlman is not persuasive.

PAGE 15/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

Accordingly, Appellants maintain that claims 2 and 14 are not unpatentable over Lewis-Weinstein in view of Perlman.

Claims 3 and 15

Since claims 3 and 15 respectively depend from claims 1 and 13, and since Appellants have argued *supra* that claims 1 and 13 are not unpatentable over Lewis in view of Weinstein, Appellants maintain that claims 3 and 15 are likewise not unpatentable over Lewis-Weinstein and further in view of Perlman.

In addition with respect to claims 3 and 15, Appellants maintain that Lewis-Weinstein and further in view of Perlman does not teach or suggest the following feature: "wherein generating the SCAC certificate includes authenticating the server name, the server public key, old certifying authority public key, **and** certifying authority name" (emphasis added) (claim 3), and similar language for claim 15. The Examiner argues that Perlman, col. 7, lines 10-12 disclose the preceding feature of claims 3 and 15.

In response, Appellants maintain that Perlman, col. 7, lines 10-12 does not disclose authenticating all four items (the server name, the server public key, old certifying authority public key, and certifying authority name) listed in clams 3 and 15. In fact, Perlman, col. 7, lines 10-12 recites: "Additionally, in system 200, the new CA 204b is configured to issue certificates in the same name as the CA 204a", which is not a disclosure of authenticating all four items (the server name, the server public key, old certifying authority public key, and certifying authority name).

PAGE 16/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

Accordingly, Appellants maintain that claims 3 and 15 are not unpatentable over Lewis-Weinstein in view of Perlman.

PAGE 17/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

GROUND OF REJECTION 3

Claim 4 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis-Weinstein and further in view of Kramer *et al.* (US Patent No. 6,324,525).

Since claim 4 depend from claim 1, and since Appellants have argued *supra* that claim 1 is not unpatentable over Lewis in view of Weinstein, Appellants maintain that claim 4 is likewise not unpatentable over Lewis-Weinstein and further in view of Kramer .

In addition with respect to claim 4, Appellants maintain that Lewis-Weinstein and further in view of Kramer does not teach or suggest the feature: "issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged".

The Examiner argues: "Lewis does not specifically disclose the usage of a Certificate Authority (CA) issuing client and server type certificates. However, Kramer discloses the method of claim 1 further comprising issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged. (see Kramer col. 105, lines 61-62; col. 105, line 66-col. 106, line 1; col. 90, lines 27-31: Certificate Authority (CA) for certificate issuance; col. 17, lines 43-47; col. 17, Lines 27-30: client and server type certificates) ... It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable the usage of client and server certificates utilizing a trusted third party designated a certificate authority for certificate issuance as taught by Kramer. One of ordinary skill in the art would be motivated to employ Kramer in order to enable secure communications over the publicly access network such as the Internet communications network. (see Kramer col. 4, lines

PAGE 18/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

19-21: "... critical that any solution utilizing the Internet for a communication backbone employ some form of cryptography ... "

In response, Appellants contend that Kramer (col. 105, lines 61-62; col. 105, line 66- col. 106, line 1; col. 90, lines 27-31; col. 17, lines 43-47; col. 17, lines 27-30) does not even come close to disclosing the preceding feature of claim 4. The Examiner has not provided any analysis to demonstrate that the Examiner's citations teach or suggest the preceding feature of claim 4.

In further response, Appellants contend that the Examiner's argument for modifying Lewis by the alleged teaching of Kramer (i.e., "in order to enable secure communications over the publicly access network such as the Internet communications network") is not persuasive because Lewis' invention already achieves secure communications over the Internet without employing the alleged teaching of Kramer.

See Lewis, col. 2, lines 6-8 ("It is, therefore, an object of the present invention to provide customer (client) to remote service provider (server) electronic transactions which are secure and reliable. "). See Lewis, col. 2, lines 23-28 ("The present invention ... is directed to an application which can be downloaded from the Internet, extracted from a zip file, installed, accessed by a pre-registered user on a **secure PC**, and used to conduct electronic commerce. "). See Kramer, col. 8, lines 11-12 ("The inbound network 110 allows a customer 2n to securely access the RSP web server 150."). Indeed, most of the Lewis disclosure is devoted to techniques for achieving secure communications over the Internet.

Therefore, a person of ordinary skill in the art would not be motivated to modify Lewis by the alleged teaching of Kramer "to enable secure communications over the publicly access network such as the Internet communications network".

PAGE 19/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

Accordingly, Appellants maintain that claim 4 is not unpatentable over Lewis-Weinstein in view of Kramer.

PAGE 20/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

GROUND OF REJECTION 4

Claim 16 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Lewis-Weinstein and further in view of Kramer *et al.* (US Patent No. 6,324,525).

Since claim 16 depend from claim 13, and since Appellants have argued *supra* that claim 13 is not unpatentable over Lewis in view of Weinstein, Appellants maintain that claim 16 is likewise not unpatentable over Lewis-Weinstein and further in view of Kramer.

In addition with respect to claim 16, Appellants maintain that Lewis-Weinstein and further in view of Kramer does not teach or suggest the following feature: "means for issuing by the certifying authority a client(CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged" (emphasis added).

The Examiner argues: "Lewis does not specifically disclose the usage of a Certificate Authority issuing client and server type certificate. However, Kramer discloses the system of claim 15, further comprising means for issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged. (see Kramer col. 105, lines 61-62; col. 105, line 66 - col. 106, line 1; col. 90, lines 27-31: Certificate Authority (CA) for certificate issuance; col. 17, lines 43-47; col. 17, lines 27-30: client and server certificates) ... It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Lewis to enable the usage of client certificates and server certificates utilizing a trusted third party designated a certificate authority for certificate issuance as taught by Kramer. One of ordinary skill in the art would be motivated to employ Kramer in order to enable secure

PAGE 21/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

communications over the publicly access network such as the Internet communications network. (see Kramer col. 4, lines 19-21)".

In response, Appellants contend that Kramer (col. 105, lines 61-62; col. 105, line 66- col. 106, line 1; col. 90, lines 27-31; col. 17, lines 43-47; col. 17, lines 27-30) does not even come close to disclosing the preceding feature of claim 16. The Examiner has not provided any analysis to demonstrate that the Examiner's citations teach or suggest the preceding feature of claim 16.

In further response, Appellants contend that the Examiner's argument for modifying Lewis by the alleged teaching of Kramer (i.e., "in order to enable secure communications over the publicly access network such as the Internet communications network") is not persuasive because Lewis' invention already achieves secure communications over the Internet without employing the alleged teaching of Kramer.

See Lewis, col. 2, lines 6-8 ("It is, therefore, an object of the present invention to provide customer (client) to remote service provider (server) electronic transactions which are secure and reliable."). See Lewis, col. 2, lines 23-28 ("The present invention ... is directed to an application which can be downloaded from the Internet, extracted from a zip file, installed, accessed by a pre-registered user on a secure PC, and used to conduct electronic commerce."). See Kramer, col. 8, lines 11-12 ("The inbound network 110 allows a customer 2n to securely access the RSP web server 150."). Indeed, most of the Lewis disclosure is devoted to techniques for achieving secure communications over the Internet.

Therefore, a person of ordinary skill in the art would not be motivated to modify Lewis by the alleged teaching of Kramer "to enable secure communications over the publicly access

PAGE 22/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

network such as the Internet communications network".

Accordingly, Appellants maintain that claim 16 is not unpatentable over Lewis-Weinstein in view of Kramer.

PAGE 23/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

SUMMARY

In summary, Appellant respectfully requests reversal of the August 11, 2004 Office Action rejection of claims 1-6 and 11-19. The Director is hereby authorized to charge and/or credit Deposit Account No. 09-0457.

Respectfully submitted,

Jack P. Friedman

Jack P. Friedman
Attorney For Appellant
Registration No. 44,688

Dated: 11/11/2005

Schmeiser, Olsen & Watts
3 Lear Jet Lane - Suite 201
Latham, New York 12110
(518) 220-1850

PAGE 24/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

RECEIVED
CENTRAL FAX CENTER
NOV 11 2005

Docket No. JP920000150US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Gupta *et al.*
Filed: 7/27/2000
Serial No.: 09/626,637
Group Art Unit: 2143
Examiner: Shin, Kyung H.
Title: METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX A - CLAIMS ON APPEAL

1. A method for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:

receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority;

verifying by the browser the original authentication certificate using the expired public key of the certifying authority; and

verifying by the browser the SCAC certificate using a new public key of the certifying authority.

2. The method of claim 1, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

PAGE 25/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate;

verifying the request by the certifying authority using the server's public key; and

generating the SCAC certificate by the certifying authority using a new private key of the certifying authority and forwarding the SCAC certificate to the server.

3. The method of claim 2 wherein generating the SCAC certificate includes authenticating the server name, the server public key, old certifying authority public key, and certifying authority name.

4. The method of claim 1, further comprising issuing by the certifying authority a client (CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged.

5. The method of claim 1, wherein the method further comprises presenting the CCAC certificate to the server during the handshake.

6. In an arrangement of networked server and browser systems conducting secure transactions and including a certifying authority for authenticating such transactions, characterized in that it includes a means for authenticating transactions when the public and private key of the said certifying authority have expired but the authentication certificates of any of server or browser systems is still valid, comprising:

PAGE 26/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

means for the server to obtain a certifying authority chain certificate using the new private key of the certifying authority,

means for presenting the said certifying authority chain certificate together with the original authentication certificate, to the browser,

means for verifying the original authentication certificate using the expired public key of the certifying authority, and verifying the certifying authority chain certificate using the new certifying authority public key by the browser.

11. The method of claim 1, further comprising accepting the transaction by the browser after said verifying the original authentication certificate and after said verifying the SCAC certificate.

12. The method of claim 1, wherein obtaining the SCAC certificate comprises using the new private key of the certifying authority.

13. A system for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:

means for receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority;

means for verifying by the browser the original authentication certificate using the

PAGE 27/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

expired public key of the certifying authority; and

means for verifying by the browser the SCAC certificate using a new public key of the certifying authority.

14. The system of claim 13, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

means for contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate;

means for verifying the request by the certifying authority using the server's public key; and

means for generating the SCAC certificate by the certifying authority using it's a new private key of the certifying authority and forwarding the SCAC certificate to the server.

15. The system of claim 13, wherein said means for generating the SCAC certificate includes means for authenticating the server name, the server public key, old certifying authority public key, and certifying authority name.

16. The system of claim 15, further comprising means for issuing by the certifying authority a client(CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged.

17. The system of claim 13, wherein the system further comprises means for presenting the

PAGE 28/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

CCAC certificate to the server during the handshake.

18. The system of claim 13, further comprising means for accepting the transaction by the browser in conjunction with said means for verifying the original authentication certificate and in conjunction with said means for verifying the SCAC certificate.

19. The system of claim 13, wherein said means for obtaining the SCAC certificate comprises use of the new private key of the certifying authority.

PAGE 29/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

RECEIVED
CENTRAL FAX CENTER
NOV 11 2005

Docket No. JP920000150US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Gupta *et al.*

Group Art Unit: 2143

Filed: 7/27/2000

Examiner: Shin, Kyung H.

Serial No.: 09/626,637

Title: METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX B - EVIDENCE

There is no evidence entered by the Examiner and relied upon by Appellants in this appeal.

PAGE 30/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20

RECEIVED
CENTRAL FAX CENTER
NOV 11 2005

Docket No. JP920000150US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Gupta *et al.*

Group Art Unit: 2143

Filed: 7/27/2000

Examiner: Shin, Kyung H.

Serial No.: 09/626,637

Title: METHOD AND SYSTEM FOR AUTHENTICATION WHEN CERTIFICATION AUTHORITY PUBLIC AND PRIVATE KEYS EXPIRE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX C - RELATED PROCEEDINGS

There are no proceedings identified in the "Related Appeals and Interferences" section.

PAGE 31/31 * RCVD AT 11/11/2005 10:50:49 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/25 * DNIS:2738300 * CSID: * DURATION (mm-ss):07-20